MINDEX CONFIDENTIAL: DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN. THIS DATA PRIVACY AND SECURITY PLAN IS CONFIDENTIAL AND SUBJECT TO THE CONFIDENTIALITY PROVISIONS OF THE LICENSE AGREEMENT BETWEEN THE PARTIES DATED SEPTEMBER 1, 2011.

1. **Data Security and Privacy Plan**
   a. **Compliance.** In order to implement all relevant state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with ESBOCES's data security and privacy policy, Contractor will:
      i. Follow policies and procedures compliant with (i) relevant state, federal, and local data security and privacy requirements, including Education Law § 2-d, (ii) this Data Security and Privacy Plan, and (iii) ESBOCES's data security and privacy policy;
      ii. Implement commercially reasonable administrative, technical, operational, and physical safeguards and practices to protect the security of Protected Data in accordance with relevant law;
      iii. Follow policies compliant with ESBOCES's Parents' Bill of Rights and the supplemental information to the agreement between Contractor and ESBOCES (the "Agreement");
      iv. Annually train its officers and employees who have access to Protected Data on relevant federal and state laws governing confidentiality of Protected Data; and
      v. In the event any subcontractors are engaged in relation to this Agreement, manage relationships with sub-contractors to contract with sub-contractors to protect the security of Protected Data in accordance with relevant law.

   b. **Safeguards.** To protect Protected Data that Contractor receives under the Agreement, Contractor will follow policies that include the following administrative, operational, and technical safeguards:
      i. Contractor will identify reasonably foreseeable internal and external risks relevant to its administrative, technical, operational, and physical safeguards;
      ii. Contractor will assess the sufficiency of safeguards in place to address the identified risks;
      iii. Contractor will adjust its security program in light of business changes or new circumstances;
      iv. Contractor will regularly test and monitor the effectiveness of key controls, systems, and procedures; and
      v. Contractor will protect against the unauthorized access to or use of Protected Data.

   c. **Training.** Officers or employees of Contractor who have access to Protected Data receive or will receive training annually on the federal and state laws governing confidentiality of such data prior to receiving access.

   d. **Subcontractors.** Contractor will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Agreement. In the event that Contractor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Agreement, it will implement policies to manage those relationships in accordance with applicable laws and will obligate its subcontractors to protect confidential data in all contracts with such subcontractors, including by obligating the subcontractor to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations and the Agreement.

   e. **Data Security and Privacy Incidents.** Contractor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, by following an incident response policy for identifying and responding to incidents, breaches, and unauthorized disclosures. Contractor will notify ESBOCES of any breaches or unauthorized disclosures of Protected Data promptly but in no event more than seven (7) days after Contractor has discovered or been informed of the breach or unauthorized release.

f. **Effect of Termination or Expiration**. Contractor will return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission at such time that the Agreement is terminated or expires.

Supplemental Information About the Agreement Between ESBOCES and Mindex Technologies, Inc.

1. **Exclusive Purpose**. Contractor will use the Protected Data to which it is provided access for the exclusive purpose of providing Contractor's services as more fully described in the Agreement. Contractor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the Agreement.

2. **Subcontractors**. In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the Agreement, Contractor will obligate its subcontractors, assignees, or other authorized persons or entities to whom it discloses Protected Data to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations, by requiring its subcontractors to agree in their contracts with Contractor to such data protection obligations imposed on Contractor by state and federal laws and regulations (e.g. Education Law §2-d) and this Agreement.

3. **Agreement Term & Termination**.
   a. The Agreement commences on the Effective Date of the Agreement and expires on the earlier of (i) Contractor no longer providing services to ESBOCES and (ii) termination of the Agreement in accordance with its terms.
   b. Contractor will return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission at such time that the Agreement is terminated or expires.

4. **Challenging Accuracy of Personally Identifiable Information**. Parents or eligible students can challenge the accuracy of any Protected Data provided by ESBOCES to Contractor by:
   a. Inquiries or complaints should be directed to the Associate Superintendent for Curriculum at your district or in writing to: Chief Privacy Officer, New York State Education Dept., 89 Washington Avenue, Albany, NY 12234; CPO@mail.nysed.gov.

5. **Data Storage and Security Protections**.
   a. **General**. Any Protected Data that Contractor receives will be stored on systems maintained by Contractor, or by a subcontractor under the direct control of Vendor, in a secure data center facility. Contractor will maintain reasonable administrative, technical and physical safeguards in accordance with 2-d to protect the security, confidentiality, and integrity of Protected Data in Contractor's custody.
   b. **Encryption**. Contractor will encrypt data in motion and at rest using methodology in accordance with Education Law § 2-d.